## 主要内容

八、无线网络安全概述（补充）

◆安全协议IEEE802.1x， IEEE802.11i

◆WEP协议安全性分析

九、安全管理

◆隐私保护

◆网络安全等级保护



## 无线网络安全

补充

## 无线网络的安全事件

◆公共免费Wi-Fi安全隐患

- 利用伪造的Wi-Fi热点，不法分子可以在几分钟之内获得上网用户的设备运行数据、网络账户、密码、照片等私密信息，甚至可以窃取用户网银资产

◆ 非法AP：未经企业许可而私自接入企业网络中的无线路由器Rogue AP

◆家用无线路由器的安全问题

- 一些路由器厂家为了日后调试和检测更方便，会在产品上保留超级管理权限。黑客可以利用这些后门直接控制路由器，进一步发起DNS劫持、窃取信息、网络钓鱼等攻击
- 通过HTTP和SSH默认端口远程访问，恶意软件的变种被注入路由器
- 密码破解
  - 无线路由器的接入密码和后台密码
  - 。。。



## 无线网络的特点

◆ 信道

- 共享，易受到监听和干扰

◆ 移动性

- 移动性带来的安全隐患

◆资源

- 移动设备中操作系统复杂，存储空间和资源有限

◆可访问性

- 一些无线设备无人值守，易受到物理攻击

## 无线网络组成

- 无线客户端
  - 一般为手机、具有Wi-Fi功能的电脑、无线传感器、蓝牙设备等
- 无线接入点
  - 提供网络或服务的连接，一般为手机基站、Wi-Fi热点、接入有线局域网和广域网的无线接入点
- 传输介质
  - 用于数据传输的无线电波




## 无线网络的安全威胁

- 密码破解
  - 破解WEP和WPA的工具已经高度集成化，破解无线网络密码的技术门槛越来越低。
- 信息泄露
  - 通过“无线嗅探”、“无线监听”、“无线会话劫持”等方式，可以轻松的窃取到其他无线用户的用户名、密码等隐私信息。
- 无线钓鱼
  - 攻击者用相同的SSID搭建一个无线网络，诱使用户进行连接，从而监控用户流量



## 无线网络的安全威胁

- 偶然连接
  - 用户被自动锁定在临近的无线接入点
- 恶意连接
  - 伪装成合法接入点
- Ad hoc网络
  - 分布式、无中心点的控制，存在安全隐患
- 非传统型网络
  - 蓝牙设备，条形码识别器，PDA，摄像头
  - 面临窃听和欺骗等安全威胁
- 身份盗窃（MAC欺诈）
  - 监听网络流量，盗用MAC
- 中间人攻击
- 拒绝服务攻击（DoS）
- 网络注入
  - 伪造配置命令，影响路由器和交换机，降低网络性能



## 无线安全措施

- 安全无线传输
  - 信息隐藏技术：取消广播服务；降低信号强度；定向天线；信号屏蔽
  - 无线传输加密
- 安全无线接入点
  - 认证
  - 基于端口的网络访问控制 IEEE802.1X
- 安全无线网络
  - 加密机制
  - 杀毒软件，防火墙等
  - 关闭标识符广播
  - 改变路由器的标识符
  - 改变预设密码
  - 只允许专用计算机访问无线网路
  - 及时升级固件和软件的漏洞

## 使用移动设备的网络

- 一个组织的网络必须适应如下情况：
  - 新设备不断增加
    - 多种终端设备
  - 基于云的应用
    - 应用可以运行在传统服务器上、云服务器、移动虚拟服务器等，各种基于云的应用和服务
  - 去边界化
    - 围绕设备、应用、用户和数据有众多网络边界
  - 外部业务需求
    - 多种接入方式和权限：访客、合作方、第三方承包方等，多种设备、多种位置接入网络



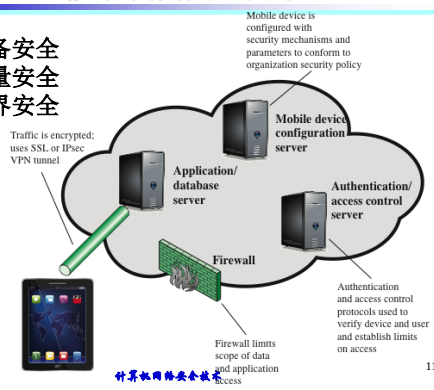
## 移动设备的安全威胁

- 缺乏物理安全控制
- 不可信移动设备的使用
- 不可信任网络的使用
- 未知来源的应用程序的使用
- 与其他系统的相互作用
  - 如云存储
- 不安全内容的使用
  - 如二维码扫描，导致移动设备访问恶意网站
- 位置服务的使用
  - 攻击者利用GPS定位功能确定位置



## 移动设备安全元素

- **设备安全**
- **流量安全**
- **边界安全**






## 移动设备安全策略

- 设备安全
  - 企业允许携带自己的设备办公（BYOD），访问企业的资源
  - 采用安全控制规则对设备进行配置
- 流量安全
  - 加密
  - 安全传输：SSL或IPv6协议
  - 虚拟私有网络VPN
  - 二层认证机制：先认证设备；再认证使用设备的用户
- 边界安全
  - 防火墙可以拦截不合法的访问
  - 对入侵检测系统IDS和入侵防御IPS 进行配置，对移动设备的数据流设置更严格的规则

# 网络访问控制
# IEEE 802.1x认证协议



## IEEE 802.1x认证协议

- IEEE 802.1x于2001年6月由IEEE正式发布，是基于端口的访问控制方案，同时还有认证和计费功能
  - 最初是为有线网络设计，2004年修订，支持无线网络WLAN的接入
  - Port based network access control protocol
- 链路层协议，在一个端口被分配IP地址之前强制进行认证
  - 核心是扩展认证协议（Extensible Authentication Protocol，EAP）
  - RFC3748



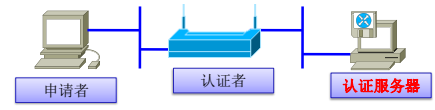
## 802.1x协议特点

- 基于端口的网络接入控制协议
  - 在设备端口上进行配置，对端口上接入的用户设备通过认证来控制对网络资源的访问
- Client/Server（C/S）结构
  - 客户端（Client）、设备端（Device）和认证服务器（Server）




## 802.1x的组成实体

- 802.1x由三个主要逻辑实体组成：
  - 客户端：
    - 申请者（Supplicant）--连接到网络的客户系统STA
  - 设备端
    - 认证者（Authenticator）--以太网交换机或者申请者试图连接的其他设备，如AP
  - 认证服务器（AS，Authentication Server）--储存申请者身份识别信息的服务器，通常是某种AAA服务器



## 客户端和设备端

- 客户端：局域网用户终端设备，如PC机，移动主机
  - 支持EAPOL（Extensible Authentication Protocol over LAN，局域网可扩展认证协议）
  - 可通过启动客户端设备上安装的802.1x客户端软件发起802.1x认证。
- 设备端：支持802.1x协议的网络设备（如交换机、无线接入点AP等）
  - 对所连接的客户端进行认证。
  - 它为客户端提供接入局域网的端口，可以是物理端口，也可以是逻辑端口（如Eth-Trunk口）。

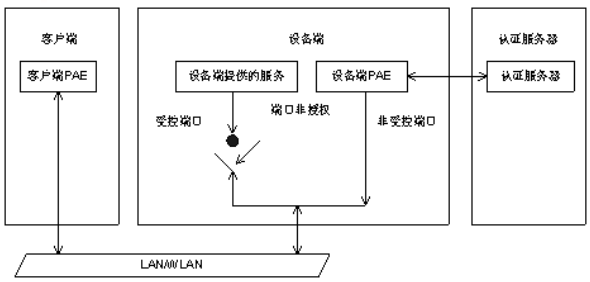


## 认证服务器

- 认证服务器：为设备端802.1x协议提供认证服务的设备
  - 实现对用户进行认证、授权和计费
  - 通常为RADIUS服务器
- 只有客户端和认证服务器需要知道EAP认证方法的细节，
- 设备端（如AP）能够将EAP消息以它理解的方式（例如RADIUS）进行封装，然后发送到认证服务器



## 受控端口和非受控端口

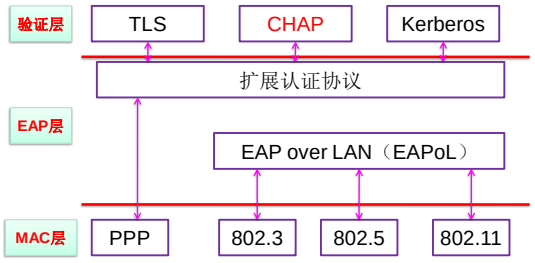





## 受控端口和非受控端口

- 在设备端为客户端提供的接入端口被划分为两个逻辑端口：受控端口和非受控端口。
  - 非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，保证客户端始终能够发出或接受认证
  - 受控端口在授权状态下处于连通状态，用于传递业务报文；在非授权状态下处于断开状态，禁止传递任何报文
- 受控方向
  - 在非授权状态下，受控端口可以被设置成单向受控：实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

## 802.1x的协议栈



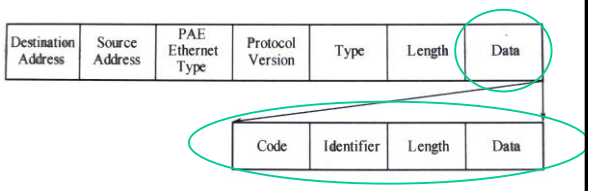



## 协议说明

- EAP
  - 可扩展认证协议 Extensible Authentication Protocol
  - EAP是一个认证框架，不是一个特殊的认证机制。EAP提供一些公共的功能，并且允许协商所希望的认证机制
  - 这些机制被叫做EAP方法。目前大约有40种不同的方法
- EAPOL
  - EAP OVER LAN，基于局域网的扩展认证协议。EAPOL是基于802.1X网络访问认证技术发展而来的。



## EAP的帧格式




- **Data域以前的部分称为EAPOL头**
- **端口实体的以太类型（PAE Ethernet Type）占两个字节，固定为16进制数0x888E**



## EAP协议介绍

- **Code域**为一个字节，表示了EAP数据包的类型，EAP的Code的值指定和意义如下：
  - **Code = 1 ————→Request**
  - **Code = 2 ————→Response**
  - **Code = 3 ————→Success**
  - **Code = 4 ————→Failure**
- **Identifier域**为一个字节，辅助进行request和response的匹配，每一个request都应该有一个response相对应，这样的一个Identifier域就建立了这样的一个对应关系，相同的Identifier相匹配
- **Length域**为两个字节，表明了EAP数据包的长度，包括Code，Identifier Length，Data域。超出Length域范围的字节应该视为数据链路层填充（padding），在接收时应该被忽略掉
- **Data域**为0个或者多个字节，Data域的格式由Code的值来决定

- EAP消息能使用多种不同格式：
  - EAP-MD5
  - EAP-TLS：基于数字证书的相互认证
  - EAP-MS-CHAP v2：基于密码的认证
  - EAP-FAST：使用隧道保护通信
  - PEAP：使用隧道保护通信，基于证书
  - …



## CHAP认证协议

- CHAP（Challenge Handshake Authentication Protocol），挑战握手认证协议
  - 是目前的在普遍使用的认证协议， RFC1994
- CHAP 协议基本过程
  - 认证者先发送一个随机挑战信息给对方，接收方根据此挑战信息和共享的密钥信息，使用单向HASH函数计算出响应值，然后发送给认证者，认证者也进行相同的计算，验证自己的计算结果和接收到的结果是否一致，一致则认证通过，否则认证失败。
  - 这种认证方法的优点即在于密钥信息不需要在通信信道中发送，而且每次认证所交换的信息都不一样。
- 使用CHAP的安全性除了本地密钥的安全性外，网络上的安全性在于挑战信息的长度、随机性和单向HASH算法的可靠性。



## CHAP认证协议

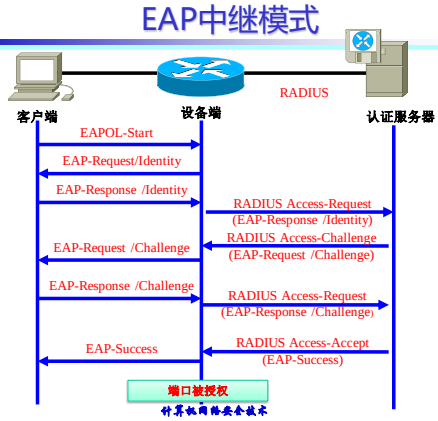



## 802.1x/EAP认证过程

- 认证过程可以由客户端发起，也可以由设备端发起
- IEEE802.1x系统支持两种认证形式：
  - EAP中继方式
  - EAP终结模式

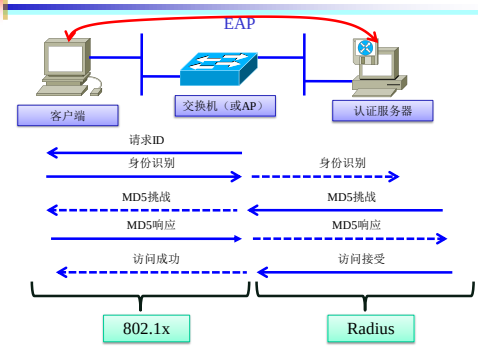
以客户端发起请求为例

## EAP中继模式






## 例：使用EAP-MD5的连接建立过程






## EAP-MD5认证过程说明--1

- 支持 IEEE 802.1x的客户端程序输入用户名和口令，发出请求认证的报文给交换机，发起连接请求。
- 交换机收到请求认证的数据帧后，向客户端发送EAP-Request/Identity。要求客户端程序发送用户名。
- 客户端收到EAP-Requst/Identity后，响应交换机的请求，回应一个EAP-Response/Identity，其中包括用户名。
- 交换机收到Response/Identity后，将该报文封装到RADIUS Access-Request报文中，发送给认证服务器



## EAP-MD5认证过程说明--2

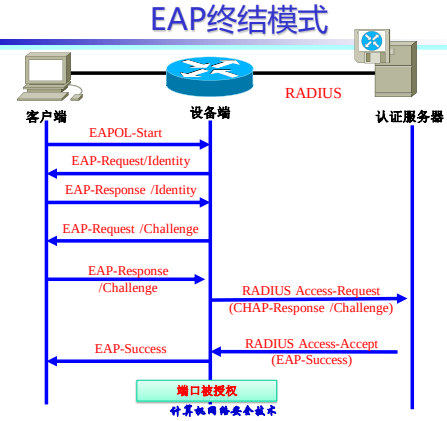
- 认证服务器接收到交换机转发的用户名信息后，产生一个Challenge，通过交换机将RADIUS Access-Challenge报文发送给客户端。
- 交换机将EAP-Request/MD5-Challenge发送给客户端，要求客户端进行认证；
- 客户端将密码和Challenge做MD5算法后的Challenged-Pass-word，在EAP-Response/MD5-Challeng回应给交换机。

## EAP-MD5认证过程说明--3

- 交换机将Challenge，Challenged Password和用户名一起送到RADIUS服务器，由RADIUS服务器进行认证.
- RADIUS服务器根据用户信息，做MD5算法，判断用户是否合法。
- 然后回应认证成功/失败报文到交换机。
  - 如果成功，携带协商参数，以及用户的相关业务属性给用户授权。如果认证失败，则流程到此结束。



## EAP终结模式






## 802.1x小结

- 优点：
  - 802.1x协议为二层协议，接入层交换机无需支持802.1q的VLAN。
  - 通过组播实现，解决其他认证协议广播问题，对组播业务的支持性好。
- 缺点：
  - 需要特定客户端软件
  - 要求楼宇交换机支持认证报文透传或完成认证过程
  - IP地址分配和网络安全问题：802.1x协议是一个2层协议，只负责完成对用户端口的认证控制，对于完成端口认证后，用户进入三层IP网络后，需要继续解决用户IP地址分配、三层网络安全等问题
  - 计费问题：802.1x协议可以根据用户完成认证和离线间的时间进行时长计费，不能对流量进行统计。



## 802.11i 协议

## 802.11 WLAN 安全性

- 无线通信的广播特性
  - 流量监测：任意在无线范围的站点均能传递信息和接收信息
- 最初的802.11 规范的安全特征
  - WEP(Wired Equivalent Privacy):有线等效保密（隐私）存在严重缺陷，易于被攻击
- 802.11i：解决WLAN的安全问题
  - Wi-Fi联盟发布无线网络保护接入WPA（Wi-Fi Alliance Wi-Fi Protected Access）：Wi-Fi网络安全存取
    - WEP到IEEE 802.11i的过渡方案
  - 最终形式：健壮安全网络（Robust Security Network，RSN）
- Wi-Fi 联盟基于WPA2的802.11i规范认证厂商设备
- WAPI（无线网鉴别和保密基础结构，我国）

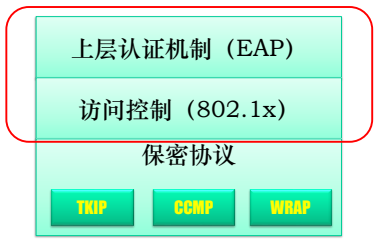


## IEEE802.11i协议的特点

- IEEE 802.11i是802.11工作组为新一代WLAN制定的安全标准，主要包括：
  - 加密技术：TKIP（Temporal Key Integrity Protocol）、AES（Advanced Encryption Standard）
  - 认证协议IEEE802.1x
    - 认证、授权和密钥管理



## IEEE 802.11i的协议结构




- **TKIP：Temporal Key Integrity Protocol，暂时密钥完整性协议**
- **CCMP**：计数器模式密码块链消息完整码协议
- **WRAP**：Wireless Robust Authenticated Protocol，无线增强认证协议



## 802.11i RSN 服务和协议：说明

- 认证 Authentication
  - 定义在用户和认证服务器AS之间交换的协议，支持相互认证，产生临时密钥，可用于无线连接的用户和AP之间。
- 访问控制 Access control
  - 强化认证功能，转发消息，密钥交换。可以支持各种认证协议.
- 消息完整性与隐私保护（Privacy with message integrity）：
  - 对MAC层数据(如 LLC PDU)和消息认证码进行加密，确保数据没有被篡改。

## 应用场景

- 两个无线工作站在同一个基本服务集内经由AP进行通信
- 两个无线工作站在ad hoc独立基本服务集内直接进行通信
- 两个无线工作站在不同基本服务集中经由各自的AP和分发系统DS进行通信
- 一个无线工作站和一个有线网络中的终端经由AP和分发系统DS进行通信



## 802.11i 的五个操作阶段：说明1

- 发现Discovery
  - AP使用信标（Beacons）和探测（Probe）通告其IEEE 802.11i安全策略.
  - 站点STA使用这些消息识别WLAN中希望与之通信的AP.
  - 站点 STA与AP进行关联，当信标和探测响应提供选择时，选择加密组件和认证机制
- 认证 Authentication
  - 站点STA 和AS相互证明各自的身份。AP在认证成功之前，阻塞STA和AP之间无认证的流量.
  - AP除了转发STA和AS之间的流量外，不参与认证 。



## 802.11i 的五个操作阶段：说明2

- 密钥生成和分发
  - AP和STA执行一系列操作，产生和分发密钥
  - 仅在AP和STA之间交换数据帧
- 保密数据传输
  - STA和终端站（目的站）之间交换数据帧。
  - 注意：安全数据传输仅在STA和AP之间进行。
  - 不提供端到端的安全性
- 连接终止
  - AP和STA交换帧。在这个阶段，安全连接被解除，连接恢复到初始状态。



## 发现阶段

- STA和AP相互确认身份，协商安全策略，建立关联。协商以下参数：
  - 保护单播通信机密性和MAC PDU完整性协议
  - 认证方法
  - 密钥管理方法
- 加密组件
  - WEP:40位或104位密钥，向后兼容
  - TKIP
  - CCMP
  - 其他
- 其他认证和密钥管理组件（AKM）

## 其他认证和密钥管理组件（AKM）

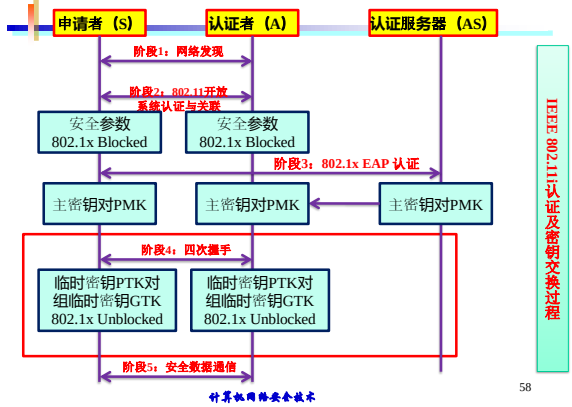
- 功能
  - 定义AP和STA之间相互认证的方法；
  - 获取根密钥
- 可选
  - IEEE802.1X
  - 预共享密钥
  - 其他
- IEEE 802.11 MPDU交换（STA和AP之间）
  - 网络和安全通道发现
  - 开放系统认证（空认证）
  - 关联



## 密钥管理阶段

- 在IEEE802.11i协议中并没有使用共享密钥作为加密和解密的密钥
- **IEEE 802.11i中的认证和密钥交换协议（AKE）**
  - **AKE协议流程与结构**
  - **四次握手协议**








## IEEE 802.11i 密钥交换过程说明

- 申请者在**网络发现阶段**发现网络接入设备及其具有的安全能力
- 申请者和认证者之间进行802.11**开放系统认证**，并通过关联请求和响应**协商**他们之间的**密码套件**
  - 没有进行实际的认证， 并且802.1x端口仍然没有打开，不能进行数据交换
- 真正的**802.1x EAP认证阶段**在申请者和认证服务器之间进行（经常使用EAP-TLS认证方案）
  - 双方进行安全的**双向认证**，并产生**主密钥对**（Pair-wise Master Key, PMK）
  - 认证服务器要通过安全信道把PMK发送给认证者

◆申请者和认证者进行**四次握手**

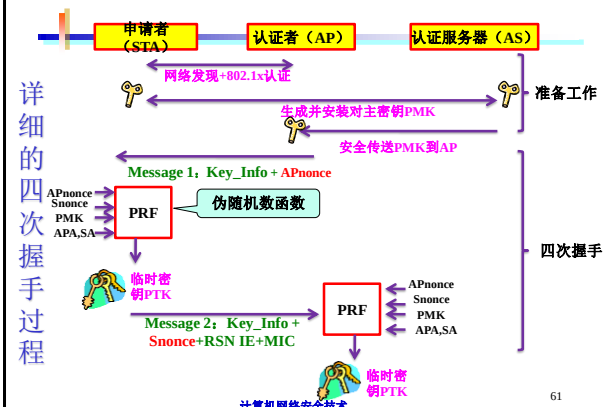
❖确认上一阶段产生的PMK的正确性和实时性

❖验证双方选择的密码组件的一致性

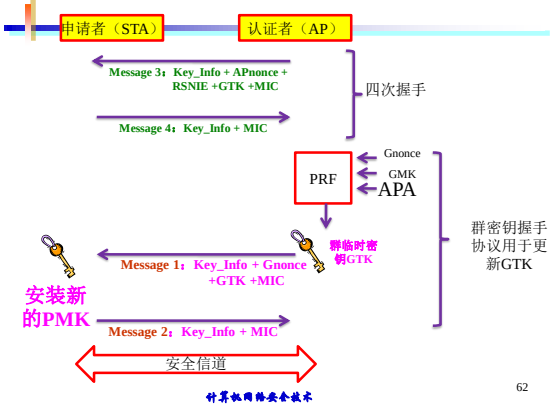
❖产生**临时密钥对PTK**和**临时群组密钥GTK**

◆最后802.1x端口（受控端口）打开，在PTK、GTK和协商的密码组件的保护下，通过数据保密协议（如CCMP）进行安全的数据通信










## 四次握手消息

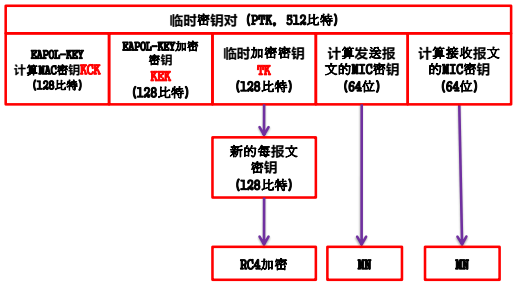
◆Message 1：AP发往STA的，消息中包含密钥信息和一个AP产生的随机数APnonce

❖STA检测通过后，产生一个随机数Snonce

❖STA将APnonce、Snonce、PMK、AP的MAC地址（APA）和STA的MAC地址（SA）输入一伪随机函数PRF，生成PTK；PTK的长度为512位，包含5部分：

1. **KCK**（Key Conformance Key）：0~127位，计算MIC（以提供四次握手和群密钥握手阶段的认证和完整性）
2. **KEK**（Key Encryption Key）：128~255位，用于四次握手和群密钥握手阶段的EAPoL帧加密密钥
3. **TK**（Temporal Key）：256~383位，STA和AP之间的普通数据加密密钥
4. **计算发送报文的MIC密钥**（64比特）
5. **计算接收报文的MIC密钥**（64比特）

◆512位的PTK，被分解成5种不同用途：






◆Message 2：STA发往AP的，消息中包含Snonce和MIC等密钥信息

- ❖AP收到消息后， 同样的方式验证并计算PTK，AP利用PTK中的KCK计算MIC并与接收到的MIC比较，如果通过验证，则构造消息3

◆Message 3：AP发往STA的，消息中包含APnonce和MIC等密钥信息；如果同时要进行GTK协商， 消息3中也可能包括GTK信息

- ❖STA收到消息后， 如果通过验证，则构造消息4

◆Message 4：消息中只包含MIC和密钥信息



◆四次握手成功以后，AP还要生成一个**256位的群组加密密钥（Group Transient Key，GTK）**：

- ❖所有与AP建立关联的STA均使用相同的GTK来发送广播消息
- ❖AP用该GTK来加密所有与之建立关联的STA的通信报文，STA则用GTK来解密由AP发送的报文并检验MAC



## IEEE 802.11i的保密机制

两种保密机制：

◆**TKIP（暂时密钥完整性协议）**

- ❖改变旧版本的 WEP协议
- ❖增加64位 消息认证码Michael message integrity code (MIC)
- ❖使用RC4加密 MPDU和 MIC值

◆CCMP（计数器模式密码块链消息完整码协议）

- ❖使用密码块链消息认证码 (CBC-MAC) 保证完整性
- ❖使用AES的计数器密码块模式CTR进行加密

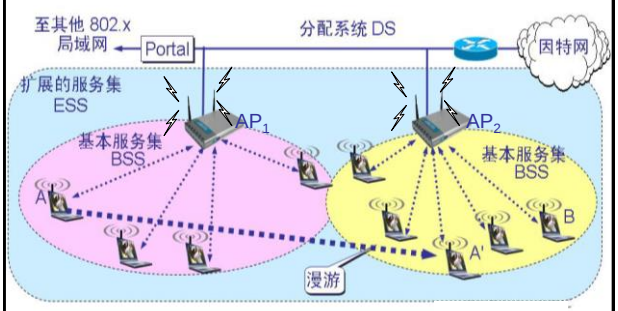
## WEP协议的安全性分析



## IEEE 802.11 无线局域网概述

- 1990年，IEEE 802.11工作组
  - 制定无线局域网WLAN的协议和传输规范
- 相关术语
  - 接入点AP
  - 基本服务集BSS
  - 协调功能
  - 分发系统 DS
  - 扩展服务集 ESS
  - MAC协议数据单元 MPDU
  - MAC服务数据单元 MSDU
  - 工作站



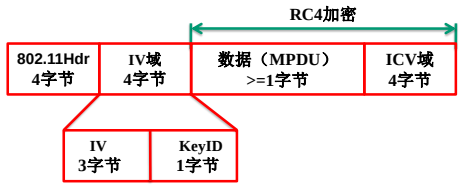





## 802.11的加密机制—WEP

- 早期无线加密机制，802.11b，1999年
- 有线等效保密WEP（Wired Equivalent Privacy）
  - 数据链路层安全协议，对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。
  - 2003年，被 Wi-Fi Protected Access (WPA) 淘汰
  - 2004年， 发布IEEE 802.11i标准（又称为 WPA2）
- 特点：认证，加密；共享密钥
- WEP的破解
  - 利用加密体制缺陷，通过收集足够的数据包，使用分析密算法还原出密码。
  - 破解WPA密码使用的是常规的字典攻击法。

## WEP帧格式

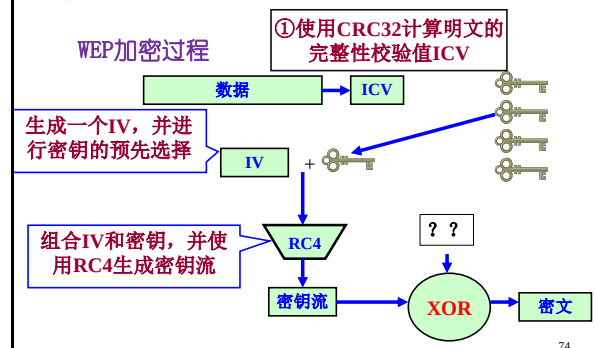



◆WEP使用预先建立的共享密钥（支持4个），具体使用哪个密钥由WEP帧中的KeyID决定

◆**IV和WEP密钥共同生成RC4算法的种子**



## 802.11的加密机制--WEP






◆问题1：为何需要计算ICV?

❖**ICV：验证数据完整性（CRC32算法）**

◆问题2：为何需要使用IV?

❖**IV：创建一个新密钥，从而避免重复使用密钥**

◆问题3：发送者应将哪些信息发送给接收者?

◆问题4：接收者如何进行解密?



## WEP的安全漏洞

◆WEP的安全漏洞

❖较小的IV空间（24bit，IV冲突）

❖IP通信中的大量已知明文

❖IV本身的弱点

❖没有密钥交换/管理机制

❖非常弱的数据完整性检查（CRC32）

❖有缺陷的身份验证系统

◆破解WEP依赖于收集大量数据（初始化向量或特定类型的数据帧）

## 说明：RC4

- **RC4**：由MIT的**Ron Rivest**于1987年设计的、可变密钥长度、面向字节操作的、使用最为广泛的序列密码之一；分析显示该密码的周期大于$10^{100}$
- **基于非线性数组变换**: 以一个足够大的数组为基础，对其进行非线性变换，产生非线性的密钥流序列
- **优点：容易用软件实现，加解密速度快**（大约比DES快10倍）



## 隐私保护



## 隐私Privacy

- 数据隐私问题 Data privacy issues
- 网络隐私问题 Network privacy issues
- 解决方案



## 什么是隐私Privacy?

- 定义：The ability to keep certain information secret
  - 拥有：Usually one’ s own information
  - 监管：But also information that is “in your custody”
  - 行为：Includes ongoing information about what you’ re doing

## 网络隐私

- Internet: 开放网络
  - 网银，电商，健康，个人身份
  - 大量敏感信息存储在计算机中，大型数据库
- 路由信息公开
  - IP 分组头部地址信息
- 加密的局限性：无法隐藏标识identities
  - 仅加密负载
  - VPN网关暴露：Even IP-level encryption (VPNs, tunnel-mode IPsec) reveals IP addresses of gateways
- 信道的广播特性
  - Wi-Fi access points



## 隐私威胁

- 明文数据传输
- 远程数据访问的安全性低
  - 数据库的远程访问
- 关联分析（大数据）
  - 多站点数据关联
  - 数据挖掘
- 位置隐私 Location privacy
  - 移动主机/手机/平板
  - 位置跟踪
- 内部威胁



## 个人数据隐私

- 什么是私有数据?
  - 身份证，出生日期，DNA记录?
  - ……
- 谁拥有私有数据?
- 个人数据泄露的后果?
  - 搜索历史；购物记录；社交网络
  - ……
- 2017年6月1日，《中华人民共和国网络安全法》正式实施
  - 网络安全法第四十四条规定：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息
  - 踪轨迹信息、通信内容、征信信息、财产信息



## 加密 和 隐私

- 数据加密：只有拥有密钥的人可以解密
- 加密能否保护数据隐私?
- 存在问题
  - 密钥管理方法?
  - 如何确定私有数据被加密?
    - 谁来保存数据？是否被加密?
    - 加密数据如何使用?
- 例：网站用户信息泄露的严重性

## 位置隐私Location Privacy

- 位置服务和位置隐私
  - 跟踪运动轨迹
- 定位方法
  - 运行商定位：使用基站信息
  - WIFI定位：基于802.11 无线信号
  - GPS定位



## 一些隐私保护的方法

- 匿名器 Anonymizers
- 洋葱路由 Onion routing
- 隐私保护的数据挖掘 Privacy-preserving data mining
- 位置隐私保护 Preserving location privacy
- 其他



## 安全管理



## 安全评估标准

- 我国的安全评估标准
  - 《计算机信息系统安全保护等级划分准则》(GB17895—1999)
  - 网络安全法（2017年6月1日正式施行）
- 美国的彩虹系列
- 欧洲信息技术安全评估规则
- 加拿大可信任计算标准
- 信息技术安全评价通用准则

## 我国的安全评估标准(GB17895-1999)

- 中华人民共和国国家标准《计算机信息系统安全保护等级划分准则》（GB17895—1999）在1999年10月经过国家质量技术监督局批准发布
- 该准则将信息系统安全分为5个等级
  - 第一级：用户自主保护级
  - 第二级：系统审计保护级
  - 第三极：安全标记保护级
  - 第四级：结构化保护级
  - 第五级：访问验证保护级



## 计算机安全保护等级

- 第一级：用户自主保护级
  - 本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。
  - 用户级别的访问控制：身份认证和防止非授权用户访问



## 计算机安全保护等级(续)

- 第二级：系统审计保护级
  - 与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。
  - 比第一级增加审计和释放后清空



## 计算机安全保护等级(续)

- 第三级：安全标记保护级
  - 本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

## 计算机安全保护等级(续)

- 第四级：结构化保护级
  - 本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。
  - 本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力



## 计算机安全保护等级(续)

- 第五级：访问验证保护级
  - 本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。
  - 为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。
  - 支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。



## 网络安全等级保护制度2.0

- 2019.5.13，网络安全等级保护制度2.0标准正式发布，实施时间为2019年12月1日。




## 等保2.0的特点

- 主要内容包括定级、备案、测评、整改与检查几个环节，并沿袭了五级分类体系
  - 主机安全、应用安全和数据安全合并为安全计算环境
  - 网络安全拆分为安全通信网络和安全区域边界，新增安全管理中心控制项。
  - 新增了个人信息保护有关的控制点
  - 强化了企业网络安全管理制度的重要性
  - 详细规定了云计算、移动互联网、物联网和工业控制系统行业（无大数据）的安全扩展要求，从主动防御、预警感知等方面增强了上述行业的网络安全性。
  - 。。。

## 《中华人民共和国网络安全法》

- 2017年6月1日起，《中华人民共和国网络安全法》正式施行
- 这是我国第一部全面规范网络空间安全管理问题的基础性法律。
- 明确了网络空间主权的原则，网络产品和服务提供者的安全义务和网络运营者的安全义务，完善了个人信息保护规则，建立了关键信息基础设施安全保护制度。



## 网络安全法的意义

- 确立了网络安全法的基本原则
  - 网络空间主权原则，网络安全与信息化发展并重原则，共同治理原则
- 提出制定网络安全战略，明确网络空间治理目标，提高了我国网络安全政策的透明度
- 进一步明确了政府各部门的职责权限，完善了网络安全监管体制
- 强化了网络运行安全，重点保护关键信息基础设施
- 完善了网络安全义务和责任，加大了违法惩处力度
- 将监测预警与应急处置措施制度化、法制化

*http://www.cac.gov.cn/2016-11/07/c_1119866583.htm*

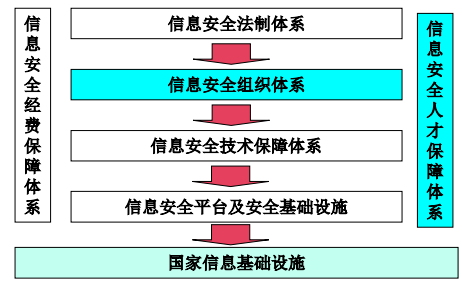


## 网络安全法要点

- 将信息安全等级保护制度上升为法律。
- 明确了网络产品和服务提供者的安全义务和个人信息保护义务。
- 明确了关键信息基础设施的范围和关键信息基础设施保护制度的主要内容。
- 明确了国家网信部门对网络安全工作的统筹协调职责和相关监督管理职责。
- 确定网络实名制，并明确了网络运营者对公安机关、国际安全机关维护网络安全和侦查犯罪的活动提供技术支持和协助的义务。
- 进一步完善了网络运营者收集、使用个人信息的规则及其保护个人信息安全的义务与责任。
- 明确建立国家统一的监测预警、信息通报和应急处置制度和体系
- 对支持、促进网络安全发展的措施作了规定。



## 国家信息安全保护框架



## 美国的彩虹系列 (Rainbow Series)

- 美国国防部在1985年公布
  - 可信计算机安全评估准则
  - Trusted Computer Security Evaluation Criteria (TCSEC)
- 为安全产品的测评提供准则和方法
- 指导信息安全产品的制造和应用



## 美国的彩虹系列 (Rainbow Series)

- 第一个信息安全评估标准，多年来它一直是评估多用户主机和小型操作系统的主要方法
- 在彩虹系列文集中，共有3种形式的文件：标准文件，解释性文件和指导性文件
- 该标准将安全分为四个方面：安全政策，可说明性，安全保障和文档
- 划分为七个安全级别，从低到高依次为D,C1,C2,B1,B2,B3,和A级



## TCSEC定义的可信计算机系统安全等级




## TCSEC的不足

- TCSEC是针对孤立计算机系统，特别是小型机和主机系统。假设有一定的物理保障，该标准适合政府和军队，不适合企业。这个模型是静态的。
- NCSC的TNI是把TCSEC的思想用到网络上，缺少成功实践的支持。
- Moore’ s Law: 计算机的发展周期18个月，现在还有可能减少到一年。不允许长时间进行计算机安全建设，计算机安全建设要跟随计算机发展的规律。

## 欧洲信息技术安全评估规则 (ITSEC)

- 首次提出信息安全的机密性、完整性、可用性概念
- 并不把保密措施直接与计算机功能相联系,而是只叙述技术安全的要求,把保密作为安全增强功能
- 把完整性、可用性与保密性作为同等重要的因素
- 定义了从E0级(不满足品质)到E6级(形式化验证)的7个安全等级
- 预定义了10种功能



## ITSEC定义了七个安全级别

- E6：形式化验证；
- E5：形式化分析；
- E4：半形式化分析；
- E3：数字化测试分析；
- E2：数字化测试；
- E1：功能测试；
- E0：不能充分满足保证。



## 如何建立网络安全机制?

补充

## 20个关键安全控制

- 美国系统网络安全协会 (SANS Institute) 在“20个关键安全控制”文档中列出了联邦组织(Federal organizations)应采用的一组核心措施以降低风险并符合联邦信息安全管理法案(FISMA)和NIST Publication 800-53的规定。
- 安全管理员将这些措施作为综合性NIST规范的组成部分，可通过达到该文档中称之为“快速胜利”的目标来实施不断演变的方案以确保综合安全。

## 20个关键安全控制

- 1. 系统设备清单
- 2. 系统软件清单
- 3. 硬件和软件的安全配置
- 4. 持续漏洞评估和修复
- 5. 防御恶意软件
- 6. 应用软件的安全性
- 7. 无线设备控制
- 8. 数据恢复能力
- 9. 安全技能评估和培训
- 10. 网络设备的安全配置
- 11. 端口、协议和服务的限制和控制
- 12. 超级用户权限的控制使用
- 13. 边界防御
- 14. 安全日志的维护、监控和分析
- 15. 基于必要性的受控访问
- 16. 帐号监测和控制
- 17. 防止数据丢失
- 18. 应急响应能力
- 19. 安全网络工程
- 20. 渗透测试



## 速战速决策略

- Install automated tools that look for devices on your network
- Active tools
  - Try to probe all your devices to see who's there
- Passive tools
  - Analyze network traffic to find undiscovered devices



## 1. 系统设备清单

- 重要性
  - If you don't know what you have, how can you protect it?
  - Attackers look for everything in your environment
  - Any device you ignore can be a point of entry
  - New devices, experimental devices, "temporary" devices are often problems
  - Users often attach unauthorized devices



## 2. 系统软件清单

- 重要性:
  - Most attacks come through software installed on your system
  - Understanding what's there is critical to protecting it
  - Important for removing unnecessary programs, patching, etc.

## 速战速决策略

- Create a list of approved software for your systems
- Determine what you need/want to have running
- May be different for different classes of machines in your environment
  - Servers, clients, mobile machines, etc.



## 3. 硬件和软件的安全配置

- 重要性:
  - Most HW/SW default installations are highly insecure
  - So if you use that installation, you're in trouble the moment you add stuff
  - Also an issue with keeping configurations up to date



## 速战速决策略

- Create standard secure image/configuration for anything you use
- If possible, base it on configuration known to be good
  - E.g., those released by NIST, NSA, etc.
- Validate these images periodically
- Securely store the images
- Run up-to-date versions of SW



## 4. 持续漏洞评估和修复

- 重要性:
  - Modern attackers make use of newly discovered vulnerabilities quickly
  - So you need to scan for such vulnerabilities as soon as possible
  - And close them down when you find them

## 速战速决策略

- Run a vulnerability scanning tool against your systems
  - At least weekly, daily is better
- Fix all flaws found in 48 hours or less
- Examine event logs to find attacks based on new vulnerabilities
  - Also to verify you scanned for them



## 5. 防御恶意软件

- 重要性:
  - Malware on your system can do arbitrary harm
  - Malware is becoming more sophisticated, widespread, and dangerous



## 速战速决策略

- Run malware detection tools on everything and report results to central location
- Ensure signature-based tools get updates at least daily
- Don’ t allow autorun from flash drives, CD/DVD drives, etc.
- Automatically scan removable media on insertion
- Scan all email attachments before putting them in user mailboxes



## 6. 应用软件的安全性

- 重要性:
  - Security flaws in applications are increasingly the attacker’ s entry point
  - Both commodity applications and custom in-house applications
  - Applications offer large attack surfaces and many opportunities

## 速战速决策略

- Install and use special web-knowledgeable firewalls
  - To look for XSS, SQL injection, etc.
- Install non-web application specific firewalls, where available
- Position these firewalls so they aren't blinded by cryptography



## 7. 无线设备控制

- 重要性:
  - Wireless reaches outside physical security boundaries
  - Mobile devices "away from home" often use wireless
  - Unauthorized wireless access points tend to pop up
  - Historically, attackers use wireless to get in and stay in



## 速战速决策略

- Know what wireless devices are in your environment
- Make sure they run your configuration
- Make sure you have administrative control of all of them
  - With your standard tools
- Use network access control to know which wireless devices connect to wired network



## 8. 数据恢复能力

- 重要性:
  - Successful attackers often alter important data on your machines
  - Sometimes that's the point of the attack
  - You need to be able to get it back

## 速战速决策略

- Back up all machines at least weekly
  - More often for critical data
- Test restoration from backups often
- Train personnel to know how to recover destroyed information



## 9. 安全技能评估和培训

- 重要性:
  - Attackers target untrained users
  - Defenders need to keep up on trends and new attack vectors
  - Programmers must know how to write secure code
  - Need both good base and constant improvement



## 速战速决策略

- Assess what insecure practices your employees use and train those
- Include appropriate security awareness skills in job descriptions
- Ensure policies, user awareness, and training all match



## 10. 网络设备的安全配置

- 重要性:
  - Firewalls, routers, and switches provide a first line of defense
  - Even good configurations tend to go bad over time
    - Exceptions and changing conditions
  - Attackers constantly look for flaws in these devices

## 速战速决策略

- Create documented configurations for these devices
- Periodically check actual devices against your standard configurations
- Turn on ingress/egress filtering at Internet connection points



## 11. 端口、协议和服务的限制和控制

- 重要性:
  - Many systems install software automatically
  - Often in weak configurations
  - These offer attackers entry points
  - If you don’ t need and use them, why give attackers’ that benefit?



## 速战速决策略

- Turn off unused services
  - If no complaints after 30 days, de-install them
- Use host-based firewalls with default deny rules on all systems
- Port scan all servers and compare against known intended configuration
- Remove unnecessary service components



## 12. 超级用户权限的控制使用

- 重要性:
  - Administrative privilege gives attackers huge amounts of control
  - The more legitimate users who have it, the more targets
    - Phishing attacks, drive-by downloads, password guessing, etc.

## 速战速决策略

- Use automated tools to validate who has administrative privileges
- Ensure all admin password/phrases are long and complex
  - Force them to change often
- Change all default passwords on new devices
  - Firewalls, wireless access points, routers, operating systems, etc.



## 速战速决策略-续

- Store passwords hashed or encrypted
  - With only privileged users allowed to access them, anyway
- Use access control to prevent administrative accounts from running user-like programs
  - E.g., web browsers, games, email
- Require different passwords for personal and admin accounts



## 速战速决策略-续

- Never share admin passwords
- Discourage use of Unix *root* or Windows *administrator* accounts
- Configure password control software to prevent re-use of recent passwords
  - E.g., not used within last six months



## 13. 边界防御

- 重要性:
  - A good boundary defense keeps many attackers entirely out
  - Even if they get in, proper use of things like a DMZ limits damage
  - Important to understand where your boundaries really are

## 速战速决策略

- Black list known bad sites or white list sites you need to work with
  - Test that periodically
- Use a network IDS to watch traffic crossing a DMZ
- Use the Sender Policy Framework (SPF) to limit email address spoofing



## 14. 安全日志的维护、监控和分析

- 重要性:
  - Logs are often the best (sometimes only) source of info about attack
  - If properly analyzed, you can learn what's happening on your machines
  - If not, you're in the dark



## 速战速决策略

- Ensure all machines have reasonably synchronized clocks (e.g., use NTP)
- Include audit log settings as part of standard configuration
  - And check that
- Ensure you have enough disk space for your logs



## 速战速决策略-续

- Use log retention policy to ensure you keep logs long enough
- Fully log all remote accesses to your machines
- Log all failed login attempts and failed attempts to access resources

## 15. 基于必要性的受控访问

- 重要性:
  - If all your machines/users can access critical data,
  - Attacker can win by compromising anything
  - If data kept only on protected machines, attackers have harder time



## 速战速决策略

- Put all sensitive information on separate VLANs
- Encrypt all sensitive information crossing the network
  - Even your own internal network



## 16. 帐号监测和控制

- 重要性:
  - Inactive accounts are often attacker's path into your system
  - Nobody's watching them
  - Sometimes even "left behind" by dishonest employees



## 速战速决策略

- Review your accounts and disable those with no current owner
- Set expiration date on all accounts
- Produce automatic daily report on all old/unused/expired accounts
- Create procedure to quickly delete accounts of departed employees

## 速战速决策略-续

- Monitor account usage to find dormant accounts (disable them eventually)
- Encrypt and move off-line all files belonging to dormant accounts
- Lock out accounts after some modest number of consecutive failed login attempts



## 17. 防止数据丢失

- 重要性:
  - Many high impact attacks are based on your data being stolen
  - You need to know when critical data is leaving your custody
  - You need to understand how and why that happens



## 速战速决策略

- Use full disk encryption
  - On all mobile devices
  - On all devices holding particularly critical data
- Other measures are more advanced



## 18. 应急响应能力

- 重要性:
  - Probably you’ll be attacked, sooner or later
  - You’ll be happier if you’re prepared to respond to such incidents
  - Can save you vast amounts of time, money, and other critical resources

## 速战速决策略

- Create written response procedures, identifying critical roles in response
- Ensure you have assigned important duties to particular employees
- Set policies on how quickly problems should be reported
- Know which third parties can help you
- Make sure you employees know what to do when there’ s a problem



## 19. 安全网络工程

- 重要性:
  - Attackers often break in at one place in your system
  - They then try to navigate to where they really want to go
  - Don’ t make that easy



## 速战速决策略

- Use a DMZ organization
  - Connect private network to DMZ with middleware
- All machines directly contacting the Internet go in the DMZ
- No machines with sensitive data should be in the DMZ



## 20. 渗透测试

- 重要性:
  - You probably screwed up something
    - Everybody does
  - You’ ll be happier finding out what if you do it yourself
  - Or have someone you trust find it

## 速战速决策略

- Regularly perform penetration testing
  - From both outside and inside your system boundaries
- Keep careful control of any user accounts and software used for penetration testing



## 应用控制规则

- Understand all 20 controls well
- Analyze how well your system already incorporates them
- Identify gaps and make a plan to take action to address them
  - 首先采用速战速决策略
  - Those alone help a lot



## 建立计划

- Talk to sysadmins about how you can make further progress
- Create long term plans for implementing advanced controls
- Think for the long haul
  - How far along will you be in a year, for example?



## 总结

- You can’t perfectly protect your system
- But you can do a lot better than most
  - And the cost need not be prohibitive
- At worst, you can make the attacker’s life hard and limit the damage
- These steps work in the real world

# 大作业提交通知

- 小组提交的作业（6月10日 20:00之前）
  - 每个小组提交程序和ppt（打包成rar或zip格式）
    （1）提交一份程序和数据，程序加注释和运行环境说明。
    （2）每组完成一份ppt（讲10分钟左右）。

6月12日课上大作业检查

- 每人提交技术报告（6月16日 20:00之前）
  - 每位同学根据大作业承担的工作独立完成并提交大作业技术报告。
  - 格式参考期刊论文要求，篇幅不限。